Security Annex

Introduction

Schiphol Nederland B.V. (SNBV) recognises that suppliers play a crucial role in ensuring the digital security of our organisation. To manage the risks of cyber threats and guarantee secure collaboration, SNBV applies specific conditions and requirements that all suppliers must comply with. These guidelines form an integral part of our contractual arrangements. Suppliers are required to adhere to the established security standards, including compliance with relevant laws and regulations, implementation of appropriate technical and organisational measures and timely reporting of security incidents.

The purpose of this Security Annex is to set out the minimum security requirements that suppliers must meet when supplying products and services to SNBV. SNBV is part of the national critical infrastructure and, as an essential entity, has a duty of care under the Cyber Security Act (*Cyberbeveiligingswet* – Cbw). In addition, SNBV is subject to the Part-IS regulations laid down by the European Union Aviation Safety Agency (EASA). The requirements set out in this Security Annex are based on recognised international standards, including ISO/IEC 27001, ISF SOGP and the NIST Cybersecurity Framework, and are consistent with these legal obligations and regulations.

Disruption of our digital processes has direct consequences for passenger safety, the continuity of air traffic and confidence in the Dutch Mainport. A significant proportion of our digital supply chain runs through suppliers, which means they are an integral part of our attack surface.

The main risk scenarios that SNBV addresses in its supplier policy include:

- Supply chain attacks, in which malicious actors gain access to the SNBV environment through a compromised update or software component from a supplier.
- Misuse of supplier accounts and remote access, for example through stolen login credentials, a lack of multi-factor authentication (MFA) or overly broad access rights granted to remote administrators.
- Ransomware and outages at the supplier, which directly impact the availability of services that are critical to SNBV's operations.
- Vulnerabilities in third-party software, firmware and hardware, including inadequate or slow patch management and the use of end-of-life components.
- Data breaches and loss of confidentiality, due to SNBV’s personal and other data or operational information being insufficiently protected when stored, processed or transmitted to sub-processors by the supplier.
- Insecure connections and integrations, such as insufficiently secured APIs, VPN connections or management interfaces between the supplier and SNBV.
- Insider threats and personnel risks in the supplier’s organisation, including inadequate screening, insufficient awareness and failure to revoke access in a timely manner on termination of employment.
- Delayed or absent incident reporting, preventing SNBV from responding in a timely manner, escalating to supervisory authorities or taking measures to limit further damage.
- Third-party and Nth-party risks, as suppliers themselves depend on subcontractors and Cloud providers operating outside the view of SNBV.

These scenarios may manifest themselves through the supply chain. Since the potential impact on airport operations, passenger safety and societal continuity is disproportionately large, SNBV places great importance on suppliers demonstrably having implemented appropriate cyber security measures. For SNBV, managing supplier risk is not merely an additional requirement but a precondition for working with suppliers.

Non-compliance with the requirements of this Security Annex may have consequences for the contractual relationship, including SNBV's right to conduct audits, suspend delivery or, in serious cases, terminate the Agreement, without prejudice to any liability of the Supplier for damage arising from non-compliance.

SNBV reserves the right to periodically update this Security Annex in response to changes in laws and regulations, new threats or evolving insights. Suppliers shall be informed about material changes through their SNBV contact

person or the SNBV website. The most recent version of this Security Annex is available at all times on the SNBV website.

The Security Annex applies to the security (including information security) of: (i) the supply of goods, Documentation, Hardware or Software; and (ii) the provision or performance of services, including SaaS or Maintenance, as assigned to [Supplier] under the Agreement, hereinafter referred to as the **'Delivery/deliveries'**.

This Security Annex forms an integral part of the Agreement between SNBV and the Supplier and comes into effect upon acceptance of the General Purchase Conditions (IT & Systems), hereinafter referred to as GPC, and/or upon the signing of the Agreement.

If SNBV and the Supplier so wish, they may agree on a customised Security Annex and include it as an annex to the Agreement or to a data processing agreement. In that case, the customised Security Annex shall replace this Security Annex.

This Security Annex shall apply for as long as the Supplier provides the Delivery/deliveries to SNBV in accordance with the Agreement and shall cease to apply upon the termination of the Agreement, without prejudice to obligations that, by their nature, extend beyond the termination of the Agreement (such as confidentiality and secure return/destruction).

The requirements in this Security Annex shall apply to the Delivery/deliveries that [Supplier] provides to SNBV, as well as to all systems, personnel, processes and environments that are used to provide or support such Delivery/deliveries or that may materially affect the security of such Delivery/deliveries. The requirements are not imposed indiscriminately on the Supplier's entire organisation but are tailored to the specific services provided and the associated risks.

Which requirements apply and how strictly they are enforced depends on the risk classification (tiering) of the relevant Delivery/deliveries. The following factors play a role in this classification: the sensitivity of the processed data, the degree of connection with the SNBV environment, the importance for business operations and the involvement of subcontractors.

However, a number of requirements apply at the organisational level because the Delivery necessarily inherits these and its security depends on them. These include requirements relating to governance and an information security management system (such as ISO 27001 certification), the security policy, personnel security, incident management and the obligation to report security incidents and data breaches.

The applicable version of this Security Annex is the version available online at the time of (i) acceptance of the GPC, or (ii) if the GPC does not apply, the signing of the Agreement. If both times apply, the earlier of the two shall prevail. SNBV shall publish each version of this Security Annex on its website, stating the effective date. All previous versions shall remain accessible in digital form, so that it is possible to determine which version applied to a specific legal relationship.

1. **Definitions**
   - 1.1. Capitalised terms used but not defined in this Security Annex have the meanings assigned to them in the Agreement and the General Purchase Conditions (IT & Systems). In addition, the capitalised terms below have the following meanings:
   - 1.2. Security Annex: this Annex pertaining to the Cyber Security Requirements and Cyber Security Measures.
   - 1.3. Cyber Security Requirements: the specific, verifiable requirements (controls/requirements) relating to information security which are set out in this Security Annex and with which the Supplier must comply.
   - 1.4. Cyber Security Measures: the organisational and technical measures relating to information security that the Supplier implements and maintains in order to comply with (i) applicable laws and regulations, (ii) the Cyber Security Requirements and (iii) the Agreement. In addition, to the extent relevant and proportionate to the execution of the Agreement, the Supplier shall apply standard industry best practices of the sector in which the Supplier operates (such as the ISO/IEC 27000 series, IEC 62443, ISAE 3402, SOC2, ISF and NIST).
   - 1.5. Cyber Security Risks: risks relating to the confidentiality, integrity and availability of SNBV's information, business assets and systems and of services provided for SNBV, and to the safeguarding of such confidentiality, integrity and availability.
   - 1.6. Self-certification (CYRA): Mapping the level of information security by means of an online self-assessment, with the option of independent certification (https://hetccv.nl/keurmerken/cybersecurity/cyra/).

2. **Supplier risk profile**
   2.1. The Supplier is obliged to cooperate with (and, if requested by SNBV, to supply information for) a risk assessment to be conducted by SNBV, on the basis of which SNBV determines the risk profile of the Deliveries. SNBV applies three (3) risk profiles:
   2.2. **Low classification:** in the case of a 'Low' risk profile, SNBV shall verify whether the Delivery to be procured complies with the Cyber Security Requirements. As supporting evidence, the Supplier shall provide SNBV upon request with at least (i) a (CYRA) self-declaration or certificate and/or (ii) a valid ISO 27001 certificate (if available). Any deficiencies identified by SNBV shall be discussed with the Supplier prior to the commencement of the service and remedied by the Supplier within a period to be determined by SNBV (following consultation), unless SNBV accepts such deficiencies in writing as an acceptable risk.
   2.3. **Medium classification:** in the case of a 'Medium' risk profile, SNBV shall verify whether the Delivery to be procured complies with the Cyber Security Requirements. Throughout the term of the Agreement, the Supplier shall hold valid certifications applicable to the Delivery/deliveries and, where appropriate, audit reports from an independent third party, namely (i) an ISO/IEC 27001 certificate or (ii) an SOC 2 report (if required by SNBV, Type II), or a certificate/report accepted in writing by SNBV as equivalent. Where the Delivery/deliveries include industrial automation and control systems (IACS), the Supplier shall also have demonstrable implementation/certification in accordance with IEC 62443 (relevant sections), as specified by SNBV. The Supplier shall supply copies of the applicable certificates/reports to SNBV. The scope thereof shall cover at least the service/product components and supporting processes relevant to the Delivery/deliveries. Any deficiencies identified by SNBV shall be discussed prior to the commencement of the service and remedied by the Supplier within a period to be determined by SNBV (following consultation), unless SNBV accepts such deficiencies in writing as an acceptable risk.
   2.4. **High classification:** in the case of a 'High' risk profile, SNBV shall verify whether the Delivery to be procured complies with the Cyber Security Requirements. Throughout the term of the Agreement, the Supplier shall hold valid certifications and/or audit reports applicable to the Delivery/deliveries, issued by an independent third party and consisting of (i) an ISO/IEC 27001 certificate or equivalent and additionally (ii) an SOC 2 Type II report or ISAE 3402 report, or an assurance report accepted in writing by SNBV as equivalent. If the Delivery/deliveries include industrial automation and control systems (IACS), the Supplier shall also have demonstrable implementation/certification in accordance with IEC 62443 (relevant sections), as specified by SNBV. The Supplier shall provide SNBV with copies of the applicable certificates and the associated audit or other reports. The scope thereof shall cover at least the service, online service and/or product and the supporting processes relevant to the Delivery/deliveries. Any deficiencies identified by SNBV shall be discussed prior to the commencement of the service and remedied by the Supplier within a period to be determined by SNBV (following consultation), unless SNBV accepts such deficiencies in writing as an acceptable risk.
   2.5. **Validity of the Agreement:** If the Supplier (i) fails to comply with a timeline established and confirmed in writing by SNBV for remedying deficiencies or (ii) cannot supply the required certifications and/or audit reports in a timely manner, or if these are no longer valid or are suspended or revoked, SNBV shall be entitled to terminate the Agreement in whole or in part after serving written notice of default and after a reasonable period for remedy has lapsed unused. SNBV shall be entitled to terminate the Agreement in whole or in part with immediate effect, without judicial intervention, if (a) the deficiency is by its nature irreparable or (b) immediate termination is reasonably necessary to mitigate security, cyber security, continuity or compliance risks. In the event of termination pursuant to this article, the Supplier shall not be entitled to any compensation or damages in respect of such termination.
   The Supplier shall demonstrate at least annually and additionally at SNBV's request that the certifications and/or audit reports referred to in the applicable risk profile are still valid.

3. **Responsibilities and compliance with Cyber Security Requirements**
   3.1. The Supplier is obliged to implement, comply with, evaluate and maintain the Cyber Security Measures at its own expense and risk during the term of the Agreement and to report on them to SNBV on request.
   3.2. The Supplier shall have a documented policy on basic cyber hygiene measures covering at least the following areas:
   - Maintenance of an up-to-date inventory of software, hardware and digital assets used in the Delivery/deliveries to SNBV;
   - Deletion or modification of factory default login credentials on all systems prior to production deployment;

- Disabling of unnecessary services, protocols and network ports on all systems used for the Delivery/deliveries;
- A procedure for secure decommissioning and data erasure of systems that are being disposed of or reused.

3.3. The Supplier shall actively ensure that its staff and any third parties involved in executing the Agreement, such as subcontractors, suppliers, advisers and financiers, comply with Cyber Security Requirements and, for this purpose, the Supplier shall provide them with a copy of the Security Annex.

3.4. The Supplier shall periodically verify and evaluate whether its undertaking and the products and/or services provided by it under the Agreement comply with the obligations arising from this Security Annex. The Supplier shall immediately inform SNBV in writing if it is unable or no longer able, or if it anticipates that it will not be able, to meet one or more obligations arising from this Security Annex during the term of the Agreement. In such a case, the Parties shall discuss whether the Supplier can implement alternative Cyber Security Measures that are acceptable to SNBV.

3.5. At SNBV's request, the Supplier shall provide written reports demonstrating that the Supplier and any third parties engaged by it in the execution of the Agreement comply with the obligations under this Security Annex.

3.6. The Supplier is responsible for preventing and managing all Cyber Security Risks that occur, or may occur, in connection with the execution of the Agreement by the Supplier. The Supplier shall deploy risk management to identify and mitigate Cyber Security Risks by implementing risk-mitigating organisational and technical Cyber Security Measures and evaluating their operation.

3.7. If the Supplier identifies a Cyber Security Risk while executing the Agreement, the Supplier shall report this to SNBV in writing no later than seven calendar days after identifying the risk concerned. This report shall include at least the following information:

a. Description of the cyber security risk;
b. A proposal for control measures to prevent, eliminate, mitigate or transfer the risk;
c. The timeframe within which the measures referred to in (b) will be implemented.

3.8. When requested to do so by SNBV, the Supplier shall support SNBV in complying with the obligations applicable to Royal Schiphol Group N.V. as a 'provider of an essential service' under the Cyber Security Act (NIS2 Directive) and the related Decree.

3.9. The Supplier shall inform SNBV in advance of any intended material changes to its information security management system (ISMS) that may affect the security, availability or aviation safety-related aspects of the Delivery/deliveries to SNBV. Material changes include:

- Change of outsourced security services (such as SOC, SIEM or incident response provider);
- Replacement or migration of Cloud infrastructure used for the Delivery/deliveries;
- Reorganisation of the structure and governance of information security within the Supplier's organisation;
- Significant changes to the scope or risk management method of the ISMS.

3.10. In the case of aviation safety-related Deliveries, the Supplier shall also notify the competent authority of material ISMS changes in accordance with IS.D.OR.255 / IS.I.OR.255 and inform SNBV about the content and timing of such notification.

4. **IT Service Management**
   4.1. The Supplier shall ensure that industry best practices relating to IT Service Management are implemented and maintained, as described in frameworks such as ITIL. Such industry best practices are intended to ensure that the Supplier's IT services are managed and delivered effectively and efficiently, in line with SNBV's requirements and expectations.

5. **Staff and engaged third parties**
   5.1. The Supplier shall ensure that all employees and third parties engaged by it who are involved in executing the Agreement, both at the commencement and during the term of the Agreement, receive training in the field of cyber security appropriate to their position and their responsibilities when performing the work in connection with the Agreement. In order to comply with this obligation, the Supplier shall in any case provide a security awareness programme, training programmes and activities based on prevailing industry best practices.
   5.2. The Supplier shall ensure that, prior to the commencement of the Agreement, a background check has been conducted on the staff and/or engaged third parties involved in executing the Agreement. These persons/organisations will only be given access to the information, business assets, systems and services of SNBV (that is/are relevant to the Agreement) if the outcome of the background check is positive. The background check must be performed in accordance with the applicable laws, regulations and ethical standards, and must also be proportionate to the nature and scope of the access that the staff concerned and/or engaged third parties will have or require to SNBV's information, business assets, systems and services.
   5.3. The Supplier shall ensure that during the term of the Agreement a formal disciplinary procedure applies to its legal relationship with staff and engaged third parties, which procedure shall specify the consequences of non-compliance with Cyber Security Requirements by a member of staff or engaged third party. The disciplinary procedure shall be drafted in accordance with prevailing industry best practice. This procedure shall in any case provide for the Supplier's power to impose the immediate suspension and revocation of access rights and privileges relating to SNBV's information and systems where there is a suspicion that the aforementioned breach is the result of wilful intent or gross negligence. The Supplier is required to report such cases in writing to SNBV without delay.

6. **Access control**
   6.1. The staff who are deployed and/or third parties that are engaged in executing the Agreement shall only have access to those parts of SNBV's information, business assets and systems as well as SNBV's service provision locations insofar as necessary to perform their tasks within the scope of their position and in connection with the Agreement (the principle of least privilege).
   6.2. The Supplier shall ensure that each account is uniquely assigned to an individual user, and not to a group or department, to allow precise tracing of user actions at all times. Group accounts and functional accounts shall not be permitted, unless SNBV has given the Supplier explicit consent for them.
   6.3. The Supplier shall maintain a list of all the staff and engaged third parties who are involved in providing the services and have access to SNBV's information, business assets and systems. During the provision of services, the Supplier shall check this list at least every 90 days to ensure that the principle of least privilege is being complied with and remaining/redundant accounts are deleted.

7. **Risk analyses, technical risk assessments and audits (Right to Audit)**
   7.1. During the term of the Agreement, SNBV shall have the right to carry out, or arrange for independent third parties to carry out, risk analyses, technical risk assessments (including penetration tests) and audits of the Supplier's service provision at its own expense. The Supplier is obliged to cooperate in these activities and to facilitate these risk analyses, technical risk assessments and audits, including by making relevant information security documents, standards, process descriptions, documentation and information available to SNBV in a timely and complete manner.
   7.2. A risk analysis, technical risk assessment or audit as referred to in paragraph 1 above shall: (a) take place no more than once a year; and (b) result in the preparation of a confidential report. SNBV shall provide the Supplier with a copy of the report.
   The Supplier shall implement, within the agreed time period, all the preventive and/or corrective actions in response to the findings identified as a result of the aforementioned risk analyses, technical risk assessments and audits.

7.3. Where the Delivery/deliveries concern activities falling within the scope of EASA Part-IS (IS.D.OR.235 or IS.I.OR.235), the Supplier acknowledges that SNBV, as the airport operator, remains at all times accountable for compliance with the applicable Part-IS obligations to the competent authority (Human Environment and Transport Inspectorate – ILT or European Union Aviation Safety Agency – EASA), even when executive tasks have been outsourced to the Supplier. The Supplier shall, upon the first request, cooperate with audits and inspections carried out by or on behalf of the competent authority in relation to the Delivery/deliveries, and shall make all necessary documentation, systems and staff available for this purpose.

8. **Network, communication and endpoint security**

8.1. The Supplier shall put in place all control measures that are necessary to protect the availability, confidentiality and integrity of data transmitted via physical or wireless networks in accordance with the most recent industry best practices, as well as to protect connected systems and applications. Appropriate control measures include, but are not confined to, Firewalls, Proxies, Intrusion Detection Systems and Intrusion Prevention Systems, network segmentation and monitoring solutions.

8.2. The Supplier shall put in place all control measures that are necessary to protect all endpoints (e.g. servers, workstations and laptops) that are used for the provision of services against malware. In that connection, the Supplier shall install for the endpoints anti-malware management software, whose signatures shall be automatically updated at least once a day, and continuously monitor it for suspicious activity.

8.3. In addition to the foregoing, the Supplier shall install for all endpoints that have access to or are used for the processing of SNBV information an Endpoint Detection and Response (EDR) or equivalent solution that provides continuous monitoring, detection of advanced attack techniques and the capability for automated or manual response (such as isolation of an endpoint). Detections that may indicate a security incident relating to the Delivery/deliveries or SNBV information shall be handled in accordance with Article 15.

8.4. The Supplier is required to use cryptographic processing to protect the data it processes. The Supplier shall apply encryption when transmitting data across networks, when storing data on portable and other devices and on removable media, such as USB sticks, and in other situations where data are vulnerable to access by unauthorised persons (such as data that can be accessed online). For this purpose, encryption shall be implemented according to the latest standards and shall be updated whenever it is determined that the existing standards no longer comply with the specified requirements:

a) Secure technologies such as the Advanced Encryption Standard (AES) technology with 256-bit or longer keys must be used for the storage of data. All keys used for this purpose must be managed in such a way that they are inaccessible to unauthorised persons and cannot be abused.

b) The Supplier shall use secured connections when accessing websites and using applications and services, so that the network traffic between the client and the web server is safeguarded from unauthorised access or modification by third parties. The Supplier shall ensure that its websites, applications and services use certificates issued by a recognised public Certificate Authority (CA), such as DigiCert. The certificate must comply with the current CA/Browser Forum Baseline Requirements for Contents of Publicly Trusted SSL/TLS Certificates. Self-signed certificates are not permitted.

9. **Passwords**

9.1. The Supplier shall ensure that the passwords of all accounts, of both administrators and users engaged by the Supplier, are stored using a secure, up-to-date one-way-hash mechanism (including unique salt).

9.2. The Supplier shall ensure that passwords for user accounts with access to SNBV data and systems are strong and comply with the guidelines and best practices as established by the National Institute of Standards and Technology (NIST SP 800-63B Guidelines). Passwords must be replaced in the event of a suspected breach or security incident. For additional access security, measures such as multi-factor authentication (MFA) and a secure password vault are recommended.

9.3. Passwords for administration accounts used by the Supplier must be at least 16 characters long and comply with the guidelines according to NIST SP 800-63B. New and existing passwords must be checked against an up-to-date blocklist of common passwords and passwords found in data breaches and must be rejected if they appear on that list. Passwords shall not be changed periodically but only in the event of a suspected breach or a security incident or if the blocklist check requires it. Preferably, the Supplier should use a Privileged Access Management (PAM) system to manage and monitor access to administration accounts.

9.4. The Supplier shall ensure that strong authentication (such as MFA) is used for (i) accounts with enhanced rights of the Supplier, (ii) access to systems processing sensitive data and (iii) remote access via the internet.
9.5. Prior approval must be obtained from SNBV if the Supplier wishes to implement alternative methods and measures to protect accounts in place of passwords.

10. **Patching & hardening**
10.1. The software used or supplied by the Supplier in executing the Agreement (OS, database, middleware and application software) shall feature all the known security patches issued by the Supplier, developer or programmer. These shall be applied or supplied in accordance with the table below when the patches are released:

Category	CVSS v3 Base score	Remediation time if internet facing	Remediation time if not internet facing
Low	0.0 - 3.9	Best effort	Best effort
Medium	4.0 - 6.9	1 month	2 months
High	7.0 - 8.9	2 weeks	1 month
Critical	9.0 - 10	Within 48 hours at the latest	2 weeks

10.2. The Supplier shall ensure hardening of the systems and software in line with the CIS benchmark hardening standards (and if these are not available, according to the Supplier's hardening standards) in order to guarantee a secure configuration.
10.3. The Supplier shall conduct periodic automatic checks for any missing patches using a tool on the systems to verify whether security patches are being implemented according to the above schedule, and shall report in relation to this.
a. Monthly reports shall be prepared detailing the status of the latest patches and hardening operations. This report shall be prepared by the Supplier and supplied to SNBV on request.
b. The report shall include information on the latest patches released, which systems have been patched and which systems are yet to be patched. In addition, information shall be provided on the hardening operations that have been carried out, which systems have been hardened and which systems are yet to be hardened.
10.4. The Supplier shall immediately notify SNBV in the event that critical vulnerabilities are discovered and additional measures shall be taken promptly to remedy these vulnerabilities.
10.5. The Supplier shall maintain a release calendar for all the software and hardware referred to above and shall anticipate end-of-life notifications by discussing an appropriate upgrade project with SNBV at least 12 months before support is due to expire.

11. **Account management**
11.1. The Supplier is obliged to use the SNBV Identity Access Management environment (SCIM-compliant) for account management in respect of the products and/or services supplied under the Agreement.
11.2. If the Supplier is unable, or no longer able, to comply with the SNBV Identity Access Management procedure, the Parties shall jointly discuss an alternative account management procedure, after which the Supplier shall submit the proposal for an alternative procedure to SNBV for acceptance. After written acceptance of this alternative by SNBV, the Supplier shall ensure that it has and maintains formal procedures for the timely creation, modification and deletion of administration and other accounts, with 'timely' in this context understood to mean within 92 calendar days.

12. **Destruction and migration of data**
12.1. In addition to the provisions in the Agreement pertaining to personal data, the Supplier shall not retain any other data obtained from SNBV under or in connection with the Agreement for longer than necessary and shall destroy such data upon the expiry of the Agreement or at SNBV's request, with due regard for the statutory retention periods.
12.2. Upon termination of the contract, physical and logical access rights to the organisation's information shall be revoked.

12.3. The Supplier is obliged to cooperate with the migration of the data to another supplier or to SNBV's own systems.

13. **Continuity**
    13.1. The Supplier shall implement all necessary IT technical measures to prevent or mitigate the loss of availability or loss of integrity of network and information systems and thereby safeguard the continuity of its obligations to provide products and/or services under the Agreement to SNBV. Appropriate measures include implementing a robust backup system to prevent data loss, establishing and regularly testing a disaster recovery and restore plan and guaranteeing the availability of sufficient and qualified staff to safeguard service provision, even in the event of illness or absence of key personnel.
    13.2. The Supplier shall put in place business continuity plans and disaster recovery arrangements relating to the Delivery/deliveries to SNBV.
    13.3. Tests shall be carried out on request on the basis of realistic scenarios corresponding to the level of importance of the Delivery/deliveries for SNBV. Scenarios shall include at least the failure of a primary data centre site, a ransomware attack and the loss of key personnel.
    13.4. Upon request, the Supplier shall provide a summary of the test results, including any identified deficiencies and the corresponding remediation plan, no later than 30 calendar days after the completion of the test.

14. **Business assets**
    14.1. Any data that may still be present on any devices of the Supplier containing storage media, such as laptops or smartphones, must be deleted by the Supplier before the device is disposed of or reused. The data must be irreversibly deleted or, if the media cannot be irreversibly deleted, the media must be irreparably and demonstrably destroyed.
    14.2. The Supplier shall ensure that sensitive data are not disclosed to unauthorised parties.
    14.3. The Supplier shall have a Bill of Materials (BOM) or a Software Bill of Materials (SBOM). If requested by SNBV, it must be possible to indicate whether specific components are used.

15. **Security incidents and reporting obligation**
    15.1. If the Supplier has identified a security incident relating to information, business assets and systems (of SNBV and/or the Supplier) or the provision of services under the Agreement, the Supplier must report this to the SNBV ICT Service Desk exclusively and immediately, and in any event within 24 hours after the Supplier became aware of such security incident.
    15.2. The Supplier must address notifications pursuant to this Security Annex to the SNBV ICT Service Desk:
    ICT Service Desk
    Tel: +31 (0)20 – 6014445
    Email: itservicedesk@schiphol.nl
    The ICT Service Desk can be contacted by phone 24 hours a day, seven days a week. If a notification is made pursuant to this Security Annex, the Supplier must also inform the contact person stated in the Agreement.
    15.3. A notification to the ICT Service Desk must contain at least the following information:
        - The start time and end time, the start date and end date and the location of the event;
        - The nature and extent of the event;
        - The department or part of the system involved in the event;
        - The time required to determine the loss and/or damage caused by the incident;
        - The nature and extent of the affected data;
        - The type and (estimated) number of data subjects, components and systems that were affected;
        - The expected consequences, including the consequences for the data subjects, components and systems, and a proposal for preventing loss and/or damage and other adverse consequences;
        - The measures that have been or will be taken to mitigate the consequences of the incident; and
        - The name and contact details of the Data Protection Officer or other contact person from whom additional information on the incident can be obtained.
    15.4. If requested by SNBV, the Supplier must permit and support an investigation of the information security incident.
    15.5. The Supplier shall provide SNBV in a timely manner with all information that SNBV requires to fulfil its own reporting obligation to the National Cyber Security Centre (NCSC) and/or the competent supervisory authority under the Cyber Security Act. The information must be reported in accordance with the schedule below:

15.6. No later than 24 hours after discovery (Early Warning): an initial report containing (i) the nature of the incident, (ii) an indication as to whether the incident is likely to be malicious in nature and (iii) whether potential cross-border consequences can be ruled out;
- No later than 72 hours after discovery (Incident Report): a detailed report containing (i) an initial impact assessment (severity and scope), (ii) available indicators of compromise (IoCs) and (iii) the systems, services and data affected;
- No later than one month after discovery (Final Report): a definitive report containing (i) a full description of the incident, including the probable cause, (ii) the measures taken and those still to be taken and (iii) the lessons learnt.
- If a security incident also constitutes a data breach within the meaning of the GDPR, the Supplier shall immediately inform SNBV, so that SNBV can also assess whether a notification to the Dutch Data Protection Authority is required within the applicable 72-hour period.

15.7. The Supplier shall provide a Single Point of Contact (SPOC), which shall be available to SNBV 24/7 in the event of a significant incident and shall be authorised to act on the Supplier's behalf with regard to the notification procedure. The Single Point of Contact shall have sufficient seniority and competence to address security issues effectively.

15.8. Where the Supplier is an organisation certified by EASA or otherwise falls within the scope of EASA Part-IS, and an information security incident related to the Delivery/deliveries to SNBV is classified by it as significant within the meaning of IS.D.OR.230 or IS.I.OR.230, the Supplier shall notify SNBV thereof without delay and in any case within 24 hours. The Supplier shall also inform SNBV as soon as it has reported such incident to the competent authority (ILT or EASA), including the content of the notification insofar as it concerns the Delivery/deliveries to SNBV. This obligation applies in addition to, and without prejudice to, the reporting obligation under Articles 15.1 to 15.7.

16. **Resources approved under the ECAC Common Evaluation Process**

16.1. Security components approved by the European Civil Aviation Conference (ECAC) and based on the 'Common Evaluation Process' (https://www.ecac-ceac.org/activities/security/common-evaluation-process-cep-of-security-equipmentare) are exempt from best practices/standards and any future changes if these would compromise the Common Evaluation Process approval. The Supplier is obliged to notify SNBV in a timely manner regarding this matter so that the Parties can agree on additional measures.

17. **Artificial Intelligence Security**

17.1. The Supplier shall determine which AI systems or applications are to be used in executing the Agreement and shall record these in an AI register, which shall be made available to SNBV on request.

17.2. The Supplier shall apply an AI security framework that includes at least the following topics:
- Risk management of AI-generated output that may affect the confidentiality, integrity or availability of SNBV information;
- Protection of training data and ML models against unauthorised access, manipulation or data poisoning;
- Periodic validation of the accuracy and reliability of AI systems deployed for security purposes.

17.3. The Supplier shall ensure that staff using AI tools to process SNBV information receive specific training on the security risks of generative AI, including the risk of unintended data transfer to external model providers.

17.4. The Supplier shall notify SNBV before deploying new or modified AI systems that process or have access to SNBV data.

18. Cryptographic Key Management and Post-Quantum Cryptography

18.1. Cryptographic keys must be protected by means of Hardware Security Modules (HSMs) or an equivalent secured key storage system. Access to keys shall be strictly limited to authorised systems and individuals in accordance with the principle of least privilege.

18.2. The Supplier shall maintain an up-to-date list of all cryptographic algorithms used to process SNBV data and evaluate annually whether these comply with current standards (including NIST, BSI, ENISA).

18.3. The Supplier shall develop and maintain a transition strategy for post-quantum cryptography (PQC) in accordance with the NIST PQC standards. The Supplier shall inform SNBV on request of the progress of the transition and make the associated roadmap available.

19. Forensic Investigation and Digital Evidence Preservation

19.1. The Supplier shall have a documented procedure for preserving digital evidence in information security incidents affecting SNBV. This procedure shall ensure the integrity and unbroken chain of custody of the evidence.

19.2. The Supplier shall support the organisation in the event of legal proceedings involving the organisation's information (e.g. requests for electronic evidence gathering (e-discovery) or forensic investigations).

19.3. If requested by SNBV after an incident, the Supplier shall ensure that relevant log files, system copies (forensic images), network capture data and authentication data are secured and retained for a period of at least 90 calendar days – or longer if legal proceedings so require.

19.4. The Supplier shall appoint a contact person responsible for forensic investigation activities and shall cooperate with forensic investigators engaged by SNBV, provided this does not contravene applicable laws and regulations.

19.5. Findings from forensic investigations shall be treated confidentially and shared solely with parties designated by SNBV.

20. Information classification and handling

20.1. The Supplier shall compile an inventory of all information resources of SNBV that it receives, processes or stores in connection with the Agreement and classify them in accordance with the classification scheme used by SNBV (or a demonstrably equivalent scheme).

20.2. The Supplier shall handle information in accordance with its classification level and apply appropriate measures for storage, transmission, access, reproduction and destruction for each classification category.

20.3. If SNBV has not provided a classification scheme, the Supplier shall use at least the following categories: Public, Internal, Confidential and Strictly Confidential, and shall apply the security measures applicable to such classifications within its own organisation.

20.4. All carriers (physical and digital) containing SNBV information at the Confidential level or higher shall be clearly marked and stored in secured environments.

21. Data Protection and Privacy

21.1. The Supplier shall process personal data that it receives or generates in connection with the Agreement solely for the purposes agreed upon in the Agreement (or data processing agreement) and in accordance with the General Data Protection Regulation (GDPR) and other applicable privacy legislation.

21.2. The Supplier shall apply the principle of data minimisation: no more personal data shall be processed than is strictly necessary for the execution of the Agreement.

21.3. If the Supplier detects a breach related to personal data (data breach notification), it shall report it to SNBV without delay – but no later than 24 hours afterwards – in accordance with Article 15, so that SNBV can assess whether the Dutch Data Protection Authority must be notified.

21.4. At SNBV's request, the Supplier shall provide information for the purpose of a data protection impact assessment (DPIA) and cooperate with the conduct of such assessment.

22. Physical Security

22.1. The Supplier shall implement appropriate physical security measures at all locations where SNBV information, systems or business assets are present or processed. Appropriate measures shall in any case include:

- Access control based on authorised identity verification (e.g. access pass, biometrics);
- Security of server rooms and data centres in accordance with the IEC 62443 or ISO/IEC 27001 standards for physical security zones;
- CCTV and alarm systems, as well as intrusion detection at critical facilities.

22.2. Access by unauthorised persons to areas where SNBV systems or data are stored must be logged and monitored. Visitors must be accompanied at all times.

22.3. The Supplier shall have measures in place to protect critical utility services (electricity, cooling) to ensure the continuity of the Delivery/deliveries.

22.4. Upon request, the Supplier shall allow SNBV to inspect the relevant physical security measures and associated audit reports.

23. Security Event Logging and Monitoring

23.1. The Supplier shall implement and maintain a central logging and monitoring solution with a central time source (NTP), which shall record all relevant security events related to the Delivery/deliveries to SNBV. Logged events shall include at least login attempts (successful and failed), configuration changes, access to sensitive data and system errors.

23.2. Where applicable, the Supplier shall record activities relating to the service provided, including at least the following details: account name, time, activity, system identification and, where applicable, network address. Activities shall include system logins and logouts, as well as failed login attempts. Transactions shall be recorded in the system.

23.3. Log files shall be protected against unauthorised modification or deletion and be retained for at least 12 months (or longer if required by applicable laws and regulations).

23.4. At SNBV's request – particularly in connection with a security incident, risk analysis or audit as referred to in Article 7 – the Supplier shall make relevant log files available in a timely manner.

23.5. The Supplier shall actively monitor security incidents and trigger escalation procedures when thresholds for suspicious activity are exceeded.

24. Secure Software Development (SDLC)

24.1. If the Supplier develops, modifies or supplies software under the Agreement, it shall apply a documented Secure Software Development Lifecycle (SSDLC) including at least:

- Security requirements based on risk analysis as an integral part of the specification phase;
- Static code analysis (SAST) and dynamic application testing (DAST) prior to each production release;
- Assessment of open-source and third-party components for known vulnerabilities (SCA – Software Composition Analysis), in accordance with the SBOM requirement set out in Article 14.3.

24.2. Critical security findings from code reviews or testing activities shall be resolved prior to production release, unless SNBV accepts a documented exception in writing.

24.3. The Supplier shall use secure development environments that are logically or physically separated from production environments.

24.4. Production data may only be used in test or development environments if such data have been anonymised or pseudonymised. Sensitive information, such as personal data, shall not be processed in a development, test and/or acceptance environment.

25. Remote Working

25.1. The Supplier shall ensure that staff and engaged third parties who have remote access to SNBV's systems or information access them only through an encrypted connection (at least TLS 1.2 or VPN with AES-256) and a hardened endpoint device managed by the Supplier.

25.2. Remote access shall be subject to strong authentication (MFA) in accordance with Article 9.4 and take place by default through the Privileged Access Management (PAM) solution managed by SNBV.

25.3. The Supplier shall have a policy for secure working from home that protects the member of staff's environment from unauthorised access to SNBV information (e.g. screen locking, use of private networks, prohibition of the use of non-approved cloud storage).

26. Nth-party (Sub-supplier) Risk Management

26.1. In addition to ***Article 3.2***, the Supplier shall have a formal programme for managing Nth-party risks (risks associated with sub-suppliers and suppliers involved in the Delivery/deliveries to SNBV).

26.2. Before the start of collaboration, the Supplier shall provide information on how it outsources tasks or engages subcontractors.

26.3. Before the start of collaboration, the Supplier shall conduct a security assessment of all critical sub-suppliers and shall repeat this assessment annually or in the event of material changes to the services provided.

26.4. Upon request, the Supplier shall inform SNBV of the names of critical sub-suppliers who have access to SNBV systems or data. SNBV shall have the right to reject a sub-supplier on the grounds of security risks, following consultation with the Supplier.

26.5. The Supplier shall include in agreements with critical sub-suppliers contractual obligations regarding information security that are at least equivalent to the obligations set out in this Security Annex.

26.6. In accordance with Article 21(2)(d) of the NIS2 Directive and the EU Implementing Regulation (C(2024)7151), the Supplier shall have a documented assessment of the cyber security risks associated with the components, software, hardware and services of its own suppliers used in the Delivery/deliveries to SNBV. The Supplier shall make a summary of this assessment available to SNBV on request.

26.7. The Supplier shall include in its own contracts with critical suppliers cyber security obligations at least equivalent to the obligations in this Security Annex and shall demonstrate this to SNBV on request. This requirement applies to suppliers who have access to SNBV data or systems, or whose products or services form an integral part of the Delivery/deliveries to SNBV.

27. **Management Responsibility and Duty of Care (NIS2 Article 20)**

27.1. The Supplier shall ensure that its board of directors or management has approved the Cyber Security Measures applied in the execution of the Agreement and shall actively monitor compliance with and the effectiveness of such measures, in accordance with Article 20 of the NIS2 Directive and the corresponding provisions of the Cyber Security Act.

27.2. The Supplier's directors and managers involved in the Delivery/deliveries must be able to demonstrate that they have completed cyber security training or education enabling them to give the approval referred to in the previous paragraph in an informed manner and to assess the relevant cyber security risks. The Supplier shall maintain records of these training courses.

27.3. At SNBV's request, the Supplier shall demonstrate compliance with the obligations in this article by submitting a statement from the management, a training certificate or equivalent proof.

27.4. If the Supplier itself is an essential or important entity within the meaning of the Cyber Security Act, the Supplier shall inform SNBV of this and provide evidence of its own registration and compliance on request.

28. Threat Intelligence and Information Sharing

28.1. The Supplier shall have a process for collecting, assessing and applying threat intelligence relevant to the Delivery/deliveries to SNBV, in order to identify threats in a timely manner and support risk-based security decisions.

28.2. The Supplier shall, without delay, share with SNBV information about threats, indicators of compromise (IoCs) or attack patterns that may be directly relevant to the Delivery/deliveries, the systems or the data of SNBV. This obligation applies in addition to the reporting obligation set out in Article 15.

29. Vulnerability management

29.1. In addition to Article 10 (Patching & hardening), the Supplier shall implement a documented vulnerability management process that provides for at least the following: (i) the periodic and automated identification of technical vulnerabilities in the systems, applications and components used for the Delivery/deliveries; (ii) risk-based prioritisation based on CVSS score and business impact; and (iii) timely remediation in accordance with the remediation times set out in Article 10.1.

29.2. The Supplier shall subscribe to relevant vulnerability alerts, such as CISA Known Exploited Vulnerabilities (KEV), NCSC-NL and supplier advisories, and shall apply these to its own Bill of Materials (see Article 14.3) in order to prioritise the resolution of known exploited vulnerabilities in components used for the Delivery/deliveries.

30. Cloud security

30.1. If the Delivery/deliveries include or rely on cloud services (such as SaaS, PaaS or IaaS), the Supplier shall inform SNBV of the identity of the underlying cloud service provider(s), the geographic location(s) where SNBV data are stored and processed and the applicable division of responsibilities (shared responsibility model).

30.2. The Supplier shall apply security measures appropriate for the Cloud model used, including at least secure configuration according to CIS Benchmarks or an equivalent standard, logical separation (tenant isolation) between SNBV data and other customers' data, management of identities and access in accordance with Articles 6 and 9 and encryption of data at rest and in transit in accordance with Article 8.4.

30.3. At SNBV's request, the Supplier shall demonstrate that the cloud environment complies with a recognised certification scheme (such as ISO/IEC 27017, ISO/IEC 27018 or CSA STAR), in addition to the certifications required in Article 2.

31. Change Management

31.1. The Supplier shall operate a documented change management process ensuring that changes to systems, applications or infrastructure supporting the Delivery/deliveries are authorised, tested and implemented in a controlled manner without jeopardising the security, availability or integrity of the services provided for SNBV.

31.2. The Supplier shall inform SNBV in advance about planned changes that may have a material impact on the manner in which the Delivery/deliveries are provided, including changes in suppliers/sub-suppliers, security functionality, authentication mechanisms, data processing locations or integrations with SNBV's systems. This obligation applies without prejudice to the reporting obligation set out in Article 3.9.

31.3. Emergency changes shall only be implemented if necessary and shall be formally reviewed and documented afterwards; SNBV must be informed as soon as possible about emergency changes affecting the Delivery/deliveries.

32. Contract termination

32.1. This article applies to any termination of the Agreement, regardless of the grounds (expiry by operation of law, notice of termination, dissolution or termination pursuant to Article 2 or any other provision of the Agreement). The Supplier shall operate a documented process for contract termination requiring at least the following: (a) timely and structured return or migration of all SNBV information and data in accordance with Article 12, in a format usable by SNBV; (b) demonstrable and irreversible destruction of any remaining SNBV information held by the Supplier and its Nth parties in accordance with Article 12, accompanied by a certificate of destruction; (c) revocation of all access rights, accounts and means of authentication granted to the Supplier and its staff and Nth parties for the Delivery/deliveries, in accordance with Articles 6 and 11; (d) transfer of knowledge, documentation and operational information relevant to continuity of service to SNBV or to a successor supplier to be designated by SNBV; (e) continued compliance with licence agreements and protection of intellectual property rights, including confidentiality, non-use and non-disclosure in respect of SNBV information, source code, designs and other protected materials, even after termination of the Agreement and for as long as the relevant rights or obligations remain in force; and (f) clearly defined retention periods for each category of data that the Supplier may retain prior to final deletion, with such retention period not exceeding that strictly necessary for the purpose for which it applies.

32.2. For the purpose of the provisions of paragraph 1(f), the Supplier shall establish the permitted retention period for each category of data (including at least personal data, SNBV’s confidential business information, log files, backups, and data that must be retained pursuant to a legal retention obligation), the legal or operational basis for that period and the manner in which deletion must be demonstrably carried out. Unless a longer period is legally required or agreed upon in writing by the parties, SNBV information is subject to a maximum retention period of ninety (90) days after the actual termination date.

32.3. The Supplier shall provide SNBV on request, and in any case no later than thirty (30) days after the actual termination date, with a written confirmation demonstrating in respect of each point (a) to (f) of paragraph 1 that the obligations set out therein have been fulfilled, including the certificate of destruction referred to in (b) and the list of retention periods referred to in paragraph 2.